End of Award Report:
Title: Privacy and trust permissions for ambient intelligence

Background

Ambient intelligence (AmI) refers to the convergence of communication technologies, computing devices, and interfaces that adapt to the needs and preferences of the user. The AmI vision is to fully computerise society and involves multiple stakeholders, delivering services and exchanging information in a timely, convenient and appropriate fashion (Bureš and Čech, 2007). One of the particular challenges of AmI is that the user will be involved in huge numbers of moment-to-moment exchanges of personal data without explicitly sanctioning each transaction. The seamless exchange of information has vast social implications and might not decrease but actually increase the complexity of life (Friedwald, et al., 2005).

The AmI vision raises its own important questions and augments the need to understand how people will trust such systems and at the same time achieve and maintain privacy (e.g. Bell and Dourish, 2007). Streitz and Nixon (2005) argue 'areas of security, privacy, and trust are critical components for the next stages of research and deployment of AmI systems.

Privacy

Privacy is a multi-dimensional construct encompassing physical and social judgments (e.g Pederson, 1999). Two types of privacy – physical and informational privacy – are particularly relevant to AmI research. Physical privacy in the anywhere, anytime, AmI society is a critical issue. Individuals will have access to information in a huge variety of environments – often while interacting with friends, family or work colleagues. The act of receiving personal information in the presence of others can be a highly stressful event, often resulting in feelings of anxiety and intimidation (Little, Briggs & Coventry, 2004).

Informational privacy is also a crucial issue for the E-Society. Privacy preferences vary considerably between users and so various architectures have been suggested that allow personalized settings e.g. Privacy Risk Model (Hong et al., 2004), Five Pitfalls for Designers (Lederer et al., 2004). Other researchers have discussed the need to understand privacy and consider issues in AmI systems related to feedback and control (Bellotti and Sellen, 1993), Fair Information Practise (Langheinrich, 2001), negotiation of boundaries (Palen and Dourish, 2003).

Trust

In discussing Ambient intelligence, the issue of trust becomes paramount. Trust is one of the most important concepts in the security arena. Unfortunately, it also remains one of the most poorly understood concepts. In an ambient world e-services will be accessible anywhere, anytime and an interesting picture is emerging about the ways in which individuals make trust judgments in technology-mediated interactions. In rapid, short-term exchanges over the Internet, for example, trust is initially secured on the basis of some emotional reaction to the look and feel of a site True, more protracted engagement is dependent upon issues such as perceived credibility and familiarity with the vendor – but trust judgments are not always made on a rational basis (Sillence et al., 2006). This raises interesting questions regarding permission setting within an AmI context – regarding the extent to which individuals should be

allowed to make day to day decisions about who or what to trust on an ad hoc basis, or should they employ agent technologies that represent their personal trust and privacy preferences and communicate these to other agents (Marsh 1994).

Personal Identity

One inevitable aspect of ubiquitous information exchange within AmI is that devices will be empowered to communicate identity information to other devices – but the whole construct of identity is complex (Schlosser, 2002). Any individual holds multiple identities and in face-to-face communication chooses to engage the identity most appropriate for that particular context. Joinson (2001) found three times as much self-disclosure in computer-mediated communication dyads compared to face-to-face pairs. However, later work (2007) suggests that this effect is reduced when people's anonymity is arbitrated through personalization technologies, particularly when a powerful audience may be viewing the disclosed material. This implies that people may well be faced with a form of generalised anxiety if and when identity detection becomes automatic. How can they be sure that their identity information is screened appropriately, so that the right information is offered at the right time?

Objectives

Prior to the start of the current project most studies of AmI technology focused on the technical limitations and constraints of such systems and ignored the social implications. The objectives of this project were (i) to involve genuine stakeholders in order to develop a set of coherent scenarios that can be used to inform policy and industry with regard to AmI development (ii) to develop a better understanding of the means by which people will seek to control their personal information (iii) a detailed analysis of general user concerns for AmI and an understanding of particular issues for those concerned about exclusion from the E-Society (iv) to document a robust set of user-generated rules concerning privacy, trust and identity permissions for AmI (v) to develop a robust model of those trust, privacy and personal identity factors that lead to information exchange within AmI contexts. All objectives have been achieved. The published work from the project explicitly addresses these issues.

Method and Results

The planned work involved four main phases in trying to further our understanding of what factors are important in controlling personal information in an ambient society. As a consequence, the method and results will be summarised for each phase:

Objectives from phase I and II

The first requirement of the project was to find a means to communicate the concept of ambient technology to the ordinary citizen. There are many potential visions of the future and so we engaged with a number of key stakeholders in order to generate specific scenarios capable of communicating something about agent technologies and the trust, privacy and identity issues they evoke. The original proposal sought to elicit information from stakeholders using the K-PRISM programme - developed to capture and formalise information flow requirements. This proved impossible, as the system relied upon the stakeholders acquiring specialist system knowledge which was impractical. However, a paper on the K-PRiSM method was presented at the annual IEEE International Carnahan Conf. on Security Technology in October 2005.

Instead, stakeholders were interviewed and asked to contribute to a detailed set of scenarios illustrating the ways in which privacy, trust and identity information might be exchanged in the future. The stakeholders included relevant user groups, researchers, developers, businesses and government departments with an interest in AmI development. Four scenarios were developed, related to health, e-voting, shopping and finance that included facts about the device, context of use, type of service or information the system would be used for.

The elicited scenarios were then given to a professional writer who produced detailed scripts for the four scenarios. These scripts were then used to develop Videotaped Activity Scenarios (or VAScs). The VASc method is a tool for generating richly detailed and tightly focussed group discussion and has been shown to be very effective in the elicitation of social rules (Little et al., 2004). VASc are developed from either in-depth interviews or scenarios, these are then acted out in context and videotaped. The VASc method allows individuals to discuss their own experiences, express their beliefs and expectations. This generates descriptions that are rich in detail and focussed on the topic of interest. For this research a media production company based in the UK was employed to recruit actors and videotape all scenarios. The production was overseen by both the producer and the research team to ensure correct interpretation. British Sign Language (BSL) and subtitles were also added to a master copy of the VASc's for use in groups where participants had various visual or auditory impairments. The development of the scenarios has been widely disseminated to interested parties and at national and international conferences. As an example, the health scenario is described in detail below. All four scenarios (health, shopping, e-voting and finance) are included in DVD format as a nominated output with this End of Award Report.

Health Scenario**:** *Bob is in his office talking on his personal digital assistant (PDA) to a council planning officer with regard to an important application deadline. Built into his PDA are several personalised agents that pass information seamlessly to respective recipients. A calendar agent records and alerts Bob of deadlines, meetings, lunch appointments and important dates. As Bob is epileptic his health agent monitors his health and can alert people if he needs help. An emergency management agent takes control in situations when a host of different information is needed; this agent has the most permissions and can contact anyone in Bob's contact list.*
Bob is going to meet his friend Jim for lunch when he trips over a loose paving slab. He falls to the ground and looses consciousness. His health agent senses something is wrong and beeps, if Bob does not respond by pressing the appropriate key on the PDA the agent immediately informs the emergency services. Within seconds the emergency services are informed of Bob's current situation and his medical history. An ambulance is on its way. Paramedics arrive, examine Bob and then inform the hospital of Bob's condition on their emergency device. The hospital staff are now aware of Bob's medical history and his present state, therefore on arrival he is taken straight to the x-ray department. A doctor receives the x-rays on her PDA. After examining Bob she confirms that he has a broken ankle, slight concussion and needs to stay in hospital overnight. After receiving treatment Bob is taken to a ward. His emergency management agent contacts John (Bob's boss) of his circumstance. The emergency management agent transfers the planning application files to John's PDA so the company do not miss the deadline. The agent also informs his parents letting them know his current state of health, exactly where he is so they can visit and that his

dog needs to be taken care of. As Bob is also head coach at a local running club the agent informs the secretary Bob will not be attending training the following week. The secretary only receives minimal information through the permissions Bob has set.

Objectives from phase III

The VASc's were shown to thirty-eight focus groups, the number of participants in each group ranged from four to twelve people (N=304). Participants were drawn from all sectors of society in the Newcastle upon Tyne area of the UK, including representative groups from the elderly, the disabled and from different ethnic sectors. Prior to attending one of the group sessions participants were informed about the aims and objectives of the study. Demographic characteristics of all participants were recorded related to: age, gender, disability (if any), level of educational achievement, ethnicity, and technical stance. As this study was related to future technology it was considered important to classify participants as either technical or non-technical (see Maguire (1998) for classification method). This was used to investigate any differences that might occur due to existing knowledge of technological systems. Therefore participants were allocated to groups initially by technical classification i.e. technical/non-technical, followed by gender, then level of educational achievement (high = university education or above versus low = college education or below), and finally age (young, middle, old). Overall this categorization process culminated in 24 main groups. Due to poor attendance at some group sessions these were run again at a later date. Although several participants with physical disabilities attended the main group sessions a group session for people with visual and auditory impairments was carried out at the Disability Forum in Newcastle. The forum was considered to have easier access and dedicated facilities for people with such disabilities.

Participants were told they would be asked to watch four short videotaped scenarios showing people using AmI systems and contribute to informal discussions on privacy and trust permissions for this type of technology. Once all the videos had been viewed an overall discussion took place related to any advantage/disadvantages, issues or problems participants considered relevant to information exchange in an ambient society. Participant's attitudes in general towards AmI systems were also noted. The duration of the sessions was approximately ninety minutes.

One objective of this project was to use the Johari Window method of disclosure within the groups. In the initial groups the method was described to participants and they were asked to evaluate each scenario in terms of disclosure windows. This method proved to be too complex and generated no extra data, therefore a decision was made to drop the procedure from further sessions and use the tool when evaluating the questionnaire in the final stages of this project.

Results

All group discussions were transcribed then read; a sentence-by-sentence analysis was employed using the Atlas.ti™ qualitative software programme. Two members of the research team coded and compared the data for consistency, good inter-rater reliability was found. The data was open coded using qualitative techniques and several categories were identified. Categories were then grouped into the different concepts; some of the main concepts were found to be multidimensional and

interrelated e.g. trust and privacy. It is difficult to summarise a rich set of qualitative data succinctly, but the overall themes are given below.

Trust
Participants expressed concerns about whether the stakeholders or their agents could be trusted to control and contain the exchange of information. The ability of individuals to interrogate the system or influence the release of personal data was a key issue. In the thematic analysis, trust was positively associated with the key constructs of *credibility, predictability* and *personalisation*.

Identity management
Identity was discussed both in terms of *disclosure preferences* and *self-reliance* incorporating issues of *autonomy* and *control.* Participants were keen to discuss the kinds of risk involved in being too open about personal matters, but also recognized that certain benefits would be denied in circumstances where disclosure was closed.

Privacy
Participants recognized *physical, informational* and *social privacy* but were also keen to discuss issues of *privacy management*. This went beyond the issue of how much information to disclose and encompassed discussion of whether or not individuals would be able to live their lives outside of the ubiquitous lens.

Social concerns
Participants commented that *exclusion* would be a major problem with adoption and use of AmI systems. People would be excluded by *age, ability, disability* and membership of *specific populations* e.g. business. Also discussed were *moral issues* related to AmI systems. Participants suggested technologies are now taking away *human responsibility*. AmI systems will further decrease social interaction, reduce our social skills and take away the concept of trust.

Scenario specific concerns
All of the main concepts emerged as important in the four scenarios, however some were considered as having greater impact. For example, *personalization* was considered to be an important concept in the health and shopping scenarios in comparison to the e-voting and finance. Participants believed *disclosure preferences* and *autonomy* (related to identity management) were more important concepts with regard to health, e-voting and finance. *Social* and *physical privacy* emerged as key concepts and associated more with the shopping, e-voting and finance scenarios and less problematic with the health. Participants envisaged the benefits of an AmI health system more in comparison to the other three scenarios.

Group specific concerns
In general, participants in the older age groups perceived AmI systems to be too *complex* and *difficult to use* in comparison to the younger age groups. However, all age groups commented setting preferences would be *time consuming* and intricate. Older adults were concerned younger people would use AmI systems for exchanging information in an ad-hoc way, in particular if used for voting in political elections. Disabled participants discussed clear advantages in terms of *independence* and *increased autonomy*. Visually impaired participants commented they often had to ask others for help in social settings

e.g. the supermarket and this can often lead to further problems, ubiquitous technologies where considered a way of having greater independence.

The qualitative data from this project is vast and in-depth analyse is ongoing to elicit themes specific to certain aspects of the proposal and certain groups. However one useful means of representing the data was provided by an adaptation of Herzberg's two-factor theory of motivation, in relation to understanding (i) those factors that must be in place to avoid dissatisfaction with the system and lead to initial acceptance subsequent uptake (Hygiene Factors) and (ii) those factors that can then motivate or de-motivate people to engage with the accepted system – relating to personal costs and benefits (Motivating Factors). In addition to these personal motivators we identified a range of social and environmental concerns that went beyond the individual. These are represented in the table below.

Hygiene Factors	**Motivating Factors**	**Social Implications**
	Benefits	
Credible	Better care	Over-reliance
Secure	Convenience	Dehumanisation
Reliable	Personalised contact	Bystander apathy
Accurate		Reduced social interaction
Transparent		Enforced participation
Context aware		Health risks
Personalised	Profile abuse	Environmental issues
Easy to use	Inflexibility	
Accessible	Increased Surveillance	
	Costs	

Table 1: Grouping and constructs associated with use of an Ubicomp system adapted from Hertzberg et al. (1959) Two Factor Theory of Motivation.

Phase IV
From the qualitative findings in Phase III a questionnaire was developed. The questionnaire was split into four main categories: health, shopping, finance and personal identity. The questionnaire was posted to all participants who took part in the focus group sessions and promoted on Zoomerang.com website. A total of 505 replies were removed from the set (mainly through incomplete answers) leaving a total of 1182 respondents: 431 health, 309 shopping, 191 finance and 281 personal identity.

Results
Of the respondents, 623 were males and 559 females. Respondents reported locations from all over the world. As might be expected, the vast majority (1013) were from the United States, 158 from the UK and 11 were from other locations. The majority fell in the 36-45 age group, though with a strong representation in all age groups from 18 to 65. Only the under 18 and over 75 groups showed any tailing off.
The majority of the sample (431) completed the health questionnaire, 161 the financial, 309 the lifestyle and 281the personal identity.

A Principal Component Analysis with Varimax rotation indicated that information exchange in AmI contexts was predicted by seven factors. They accounted for 68% of

the total variance and each had an eigenvalue index greater than 1.0. The interpretation of the factors was based on the grouping of variables from the original questionnaire.

Factor 1: Security of information, privacy (informational, physical, social) and surveillance
Factor 2: Trust through credibility, responsibility and personalisation
Factor 3: Design of system in relation to complexity, reliability and human values
Factor 4: Social concerns in relation to control and physical privacy
Factor 5: Benefits of using AmI systems
Factor 6: Data management in relation to verification and access to information
Factor 7: Privacy preferences

This was used in a subsequent regression analyse to develop a model of trust, privacy and personal identity factors that lead to information exchange within AmI contexts: health, finance, lifestyle and personal identity.

Health model
Security (20.5%), design (3.3%), trust (1.4%), data-management (1.2%) and benefit (.7%) were all found to be predictive factors for exchanging health information in AmI contexts ($F\ 5, 1176 = 18.66$, $p<0.001$).

Finance model
Security (24.1%), trust (.6%), data-management (1.4%) and benefit(1%) were all found to be predictive factors for exchanging health information in AmI contexts ($F\ 4, 1177 = 23.32$, $p<0.001$).

Personal identity model
Security (18.9%), design (3%) and data-management (1.6%) were all found to be predictive factors for exchanging identity information in AmI contexts ($F\ 3, 1178 = 22.91$, $P<0.001$).

Lifestyle model
Social (16.3%), design (3.1%), security (1.7%) and trust (2.5%) were all found to be predictive factors for exchanging health information in AmI contexts ($F\ 4, 1177 = 17.286$; $p<0.001$).

The questionnaire warrants further development due to the low variance explained in each of the models.

Disclosure preferences
On the questionnaire participants completed two disclosure grids: one grid related to who they were happy revealing personal information to e.g. doctor, partner and the other grid related to who currently had access to that particular information. A method based upon Johari windows was used to investigate the relationship between current access and disclosure preferences. The results from this study indicated no correlation between disclosure preferences and actual disclosure patterns – indicating that people leak information in an unprincipled manner.

Activities

The research team took a full role in all of the *e-society* programme activities and also organised or took a major role in organising a number of workshops and engaged in dissemination through other sources.

Workshops and other sources:

(i) A workshop on Social Aspects of Computing Technologies was organised by the proposer and Dr Linda Little (lead researcher on the project) and Dr Elizabeth Sillence (lead research on Professor Briggs' other E-Society project – Bodies Online). This was held at Northumbria University on November 8th 2004

(ii) Professor Briggs co-organised a workshop 'Considering trust in ambient societies' at the leading international conference in human-computer interaction (CHI). An overview was given of both this and Prof. Briggs' other E-Society project, details as follows: Little, L. & Sillence, E. (2004). Trust & Privacy in the Ambient World. In Proceedings of the ACMSigCHI Workshop on considering trust in ambient societies, ACM Press, April 2004, Vienna, Austria

(iii) Professor Briggs and Dr Linda Little organised a workshop entitled 'Privacy, Trust and Identity Issues for Ambient Intelligence' which was held at Pervasive, Dublin, Ireland, 4th International Conference on Pervasive Computing May 7th, 2006

(iv) A panel session was held at the British HCI Conference in Edinburgh, September, 2005 entitled 'Ambient Intelligence: Does Private Mean Public?' This panel was organised by Professor Briggs, Dr Linda Little and colleagues form other academic institutions, industry and a member who works for the Canadian Government.

(v) The following paper was presented at a workshop on Ambient Intelligence, Interact, Rome, September 2005: Little, L & Briggs, P. (2005). Designing Ambient Intelligent Scenarios to Promote Discussion of Human Values

(vi) Dr Linda Little was invited to present work from the project at the Disability North East and Codeworks monthly meetings.

(vii) The following paper was presented at a workshop on Privacy and HCI, CHI Conference, Montreal, Canada, April, 2006: Little, L., & Briggs, P. (2006). Investigating privacy in an ambient world.

(viii) A workshop on the Family and Communication Technologies was organised by the proposer and Dr Linda Little (lead researcher on the project) and Dr Elizabeth Sillence (lead research on Professor Briggs' other E-Society project – Bodies Online). This was held at Northumbria University on May 27th, 2007. The output from the workshop is a special issue on Family and Communication Technologies to appear in the International Journal of Human Computer Studies.

Outputs

DVDs of Scenarios

Peer-Reviewed Journals and Book Chapters

Kostakos, V., O'Neill, E., Little, L and Sillence, E. (2005). The Social Implications of Emerging Technologies. *Interacting with Computers*, 17, 475-483.

Little, L., Storer, T., Briggs, P., & Duncan, I. (in press). E-voting in an AmI world: Trust, privacy and social implications. *Social Science Computer Review*, December 2007

Little, L., Marsh, S., & Briggs, P. (2006). Trust and privacy permissions for an ambient world. In R. Song, L. Korba, G. Yee (Eds.) *Trust in e-services: technologies, practices and challenges*. Hershey: The Idea Group.

Little, L., Briggs. P. (under review) Ubiquitous Computing and Disability: exclusive or inclusive systems? Submitted to *Information, Technology and People*.

Peer-reviewed conference papers

Little, L., & Briggs, P. (2007). Ubiquitous computing: privacy problems with emerging technologies. *International Crime Science Conference*, London July 2007.

Little, L. & Briggs, P. (2006). Using AmI systems for exchanging health information: Considering trust and privacy issues. *E-Society Conference*, September 2006

Briggs, P., Little, L., Love, S., Marsh, S., & Coventry, L. (2005). Ambient Intelligence: Does Private Mean Public? *British Computer Society: Human-Computer Interaction Conference* Edinburgh, September 2005.

Briggs, P. and Marsh, S. (2006). Trust, forgiveness and regret: a psychological model? Paper presented at Workshop on Trust, Privacy and Identity Issues for Ambient Intelligence. *Pervasive '06: The Fourth International Conference on Pervasive Computing*, Dublin.

Little, L., & Briggs, P. (2006). Tumult and turmoil: privacy in an ambient world. Paper to be presented Workshop on Privacy, trust and identity issues for ambient intelligence. *Pervasive '06: The Fourth International Conference on Pervasive Computing*, Dublin.

Little, L., & Briggs, P. (2006). Investigating privacy in an ambient world. Paper presented at workshop on Privacy and HCI, *CHI 2006*, Montreal, Canada.

Little, L & Briggs, P. (2005). Designing Ambient Intelligent Scenarios to Promote Discussion of Human Values. Paper presented at Ambient Intelligence workshop, *Interact,* Rome, September 2005.

Marsh, S., Briggs, P. and Wagealla, W. (2004). Considering Trust in Ambient

Societies. In: *Extended Abstracts of CHI 2004*, (pp 1707-1708). New York: ACM Press.

Storer, T., Little, L., & Duncan, I. (2006). An exploratory study of voter attitudes towards a pollsterless remote voting system. In *IaVoSS Workshop on Trustworthy Elections (WOTE 06) Pre-Proceedings* (D. Chaum, R. Rivest, and P. Ryan, eds.), (Robinson College, University of Cambridge, England), pp. 77-86, June 2006.

Impacts

A number of large organisations have shown an interest in our work. For example, we were invited to speak about this work to Microsoft in relation to their involvement in the Connecting for Health agenda (and they requested and received a DVD of the health scenario). We have been collaborating with IBM (USA) in relation to the 'disclosure windows' concept, exploring technologies to record the kinds of disclosure preferences we reported in Phase IV. We were also invited to speak to a consortium of people interested in e-voting and to comment on the 'pret-a-voter' system at Newcastle University (they also requested and received a copy of our e-voting DVD). Finally, we have been asked to submit details of our work to the Home Office in relation to concerns about e-inclusion.

Future Research Priorities

We have assessed the trust, privacy, disclosure and identity concerns of various groups of individuals – including older adults, ethnic minorities and disabled groups and have begun to disseminate these findings. We have also developed new tools to express disclosure preferences and have entered discussions with commercial organisations in respect of these. Our findings are important when we consider the social and technological agenda thrown up by the introduction of UK identity cards and other forms of federated identity. To date, most high-level discussions of such issues have focussed on government policy, however we know that individuals are increasingly relaxed about sharing information through the Internet and as yet we have not properly tried to reconcile the behaviours and concerns of the individual with the demands of the state and the multi-media corporation. In trying to influence this agenda, we have played an active part in a number of high-level workshops aimed at identifying future issues in privacy and security. For example, Professor Briggs was invited to participate in the following workshops:
'*A fine balance - encouraging technology and protecting privacy*' held at the Royal Society, 8 November 2006; The Oxford Internet Institution workshop on Emerging Forms of Personal Identification and Identity Management in e-Government Service Relationships with the Citizen: Comparing Developments and Learning Lessons from Canada, USA and UK, 29 September 2006; and participated in the DTI (Technology Strategy Board) event **-** *Ensuring privacy and consent in identity management infrastructures,* London, July 10th 2007. The latter event took a clear stance in wishing to reconcile the social science and technology perspectives in order to achieve human-centred solutions. We are one of only two research groups in the UK that have explicitly tried to use psychological models of trust, privacy, identity and security in order to inform policy and technology development, but the question of how to balance the psychological needs of the individual with the identity and security needs of the organisation and the state has become a crucial topic for our generation.

Ethics

All studies had prior approval from Northumbria University Ethics Committee.

References

Bell, G. & Dourish, P. (2007). Yesterday's tomorrows: notes on ubiquitous computing's dominant vision. *Pers Ubiquit Comput* 11: 133–143

Bellotti, V., Sellen, A. (1993). Design for Privacy in Ubiquitous Computing Environments. *Proc. ECSCW '93*, Kluwer A.P., Dordrecht, The Netherlands

Bureš, V. & Čech, P. (2007). Complexity of Ambient Intelligence in Managerial Work. *ITiCSE'07*, Dundee, Scotland, United Kingdom.

Friedewald, M., Costa, O., Punie, Y., Alahuhta, P., Heinonen, S. (2005). Perspective of ubiquitous computing in the home environment. *Telematics Information*, 22 (3), 221-238

Hong, J.I., Ng, J.D., Lederer, S. & Landay, J. (2004). Privacy risk models for designing privacy-sensitive ubiquitous computing systems, *Proceedings of the 2004 conference on Designing interactive systems: processes, practices, methods, and techniques*, Cambridge, MA, USA

Joinson, A. N. (2001). Self-disclosure in computer-mediated communication: The role of self-awareness and visual anonymity. *European Journal of Social Psychology*, 31, 177-192.

Joinson, A.N., Woodley, A., & Reips, U-R. (2007). Personalization, authentication and self-disclosure in self-administered Internet surveys. *Computers in Human Behavior*, 23, 275-285.

Langheinrich, M. (2001). Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems, *Proceedings of the 3rd international conference on Ubiquitous Computing*, p.273-291, September 30-October 02, Atlanta, Georgia, USA

Lederer, S., Hong, J.I. Dey,K., & Landay,A. (2004). Personal privacy through understanding and action: five pitfalls for designers, *Personal and Ubiquitous Computing*, v.8 n.6, p.440-454,

Little, L., Briggs, P., & Coventry, L. (2004). Videotaped Activity Scenarios and the Elicitation of Social Rules for Public Interactions. *British Human Computer Interaction Conference*, Leeds

Maguire, M.C. (1998). A Review of User-Interface Guidelines for Public information kiosk Systems. *International journal of Human-Computer Studies*, 50. 263-286

Marsh, S. (1994). *Formalising Trust as a Computational Concept*. PhD Thesis, University of Stirling, Scotland. Available online via www.stephenmarsh.ca

Palen, L. & Dourish, P. (2003). *Unpacking "Privacy" for a Networked World*. CHI Letters,. 5(1): p. 129--136.

Pedersen, D.M. (1999). Model for types of privacy by privacy functions. *Journal of Environmental Psychology*, 19. 397-405.

Schlosser, F. (2002). So, how do people really use their handheld devices? an interactive study of wireless technology use. *Journal of Organizational Behaviour*, 23, 401–423.

Sillence, E., Briggs, P. Harris, P, Fishwick, L. (2006). A framework for understanding trust factors in web based health advice. *International Journal of Human Computer Studies,* 64 (8), 697-713.

Streitz, N., & Nixon, P. (2005). The disappearing computer. *Communication of the ACM, 48, 3,* 32-35